IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,	Case No. 3:18 CR 435
Plaintiff,	MEMORANDUM OPINION SUPPLEMENTING PRIOR ORDER (DOC. 28)
-vs-	
Michael S. Crawford,	JUDGE JACK ZOUHARY
Defendant.	

INTRODUCTION

In August 2018, Defendant Michael Crawford was indicted for receipt and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) (Doc. 1). The charges stem from searches of his two Google accounts and his Synchronoss account. Both Google and Synchronoss detected child pornography on their platforms and sent tips to the National Center for Missing and Exploited Children (NCMEC). NCMEC, in turn, forwarded these tips to law enforcement, which executed search warrants on the accounts in February 2018.

Crawford moved to suppress evidence obtained from the accounts (Doc. 20). The Government responded (Doc. 23), and Crawford replied (Doc. 26). This Court held a Record Hearing in February 2019 and denied Crawford's Motion (Doc. 28). This Opinion follows.

BACKGROUND

NCMEC is a private, nonprofit organization that works to reduce child sexual exploitation (Doc. 24-10 at ¶ 2). It operates a national clearinghouse for investigative tips about online child exploitation called the CyberTipline (*id.* at ¶ 5). The CyberTipline allows electronic-service providers -- like Google and Synchronoss -- to report online, child-exploitation activity (*id.*).

Google Accounts

Google provides a variety of online services, including email and cloud storage. To create an account and use Google applications, users must agree to Google's Terms of Service. The Terms prohibit use of Google applications in violation of the law and state that Google "may review content to determine whether it is illegal" (Doc. 24-11 at 4).

Google, using hashing technology, scans files uploaded to its platform for suspected child pornography (Doc. 23 at 16). After a Google employee views an image and determines it to be child pornography, the image is given a digital fingerprint -- or hash -- and is added to a database with other hashes corresponding to apparent child pornography. *See United States v. Miller*, 2017 WL 2705963, at *2–3 (E.D. Ky. 2017). *See also* Richard Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38–41 (2005) (discussing hashing technology). When a user later uploads a file matching a known hash, Google confirms the image is child pornography and then reports it to NCMEC in the form of a CyberTip (Doc. 24-11 at ¶ 7).

Here, from August to September 2014, Google sent three CyberTips to NCMEC stating that child-pornography images were recently uploaded to a Google account named countrywidetransportservices@gmail.com (*see* Doc. 24 at ¶ 22). The CyberTips included the account's secondary email address, countrywide2007@aol.com (*see* Doc. 24-2 at 6). The images were not attached to an email but rather were uploaded to Google's photo-sharing application, Google+ Photos (*id.* at 7). A Google employee viewed the images and determined they were child pornography before sending the CyberTips to NCMEC (*id.*).

After receiving the CyberTips, NCMEC investigated. NCMEC first viewed the images and confirmed they were child pornography (*id.* at 10). Next, through searches of publicly available

information, NCMEC determined Crawford owned a business near Lima, Ohio, called Countrywide Transport Services, with an email address of countrywidetransportservices@gmail.com (*id.* at 11).

Google suspended countrywidetransportservices@gmail.com due to the apparent child-pornography activity. Shortly after that account was suspended, a new account, countrywidetransportservicesOH@gmail.com, was created. This new account registered with the same secondary email address as the suspended account (Doc. 24 at ¶¶ 22–23).

One year later, in September 2015, Google detected 21 child-pornography images uploaded to Google+ Photos by countrywidetransportservicesOH@gmail.com. Google viewed the suspected content and sent another CyberTip to NCMEC (Doc. 24-3 at 8–14; *see also* Doc. 24-11 at ¶ 11). NCMEC linked this latest CyberTip to the three earlier ones from 2014 (Doc. 24-10 at ¶¶ 24, 28, 39). NCMEC searched publicly available information using countrywide2007@aol.com and found Facebook and MeetMe accounts in Crawford's name (Doc. 24-3 at 19–20). It also found several phone numbers associated with Crawford and Countrywide Transport Services (*id.* at 21–22).

NCMEC forwarded tips of Crawford's suspected activity to the Cuyahoga County Prosecutor's Office (Doc. 24-10 at ¶ 33). But due to the large number of tips that office receives, that office mistakenly failed to act on the tips (Doc. 24-7 at ¶ 7).

Synchronoss Account

Synchronoss manages cloud-storage accounts linked to Verizon cell phones. Verizon subscribers can use Synchronoss accounts to back up their phone contents and to store photos and videos (Doc. 23 at 3). The Synchronoss Terms of Service, which users must acknowledge before using the service, bar illegal content and state that Synchronoss may monitor content uploaded to the accounts (*id.*).

Like Google, Synchronoss uses hashing technology to detect suspected child pornography (Doc. 24-12 at ¶ 3). But unlike Google, where employees confirm that images are child pornography before sending CyberTips to NCMEC, the Synchronoss system is automated. "Once files are flagged as being potentially identified as child pornography, Synchronoss reports the information to [NCMEC]" (*id.*). "Synchronoss does not view any of the flagged files . . . and does not conduct any other type of review of the customer's account or storage" (*id.*).

Here, in October 2017 and January 2018, Synchronoss sent three CyberTips to NCMEC after detecting several uploads of suspected child-pornography images to one of its cloud-storage accounts (Docs. 24-4; 24-5; 24-6). Synchronoss did not view the images before reporting them to NCMEC, and NCMEC, in turn, did not view them either (Docs. 24-4 at 1; 24-5 at 1; 24-6 at 1). The CyberTips provided the uploading device's phone number, which matched one that NCMEC had earlier linked to Crawford (Docs. 24-4 at 3, 5; 24-5 at 3, 6; 24-6 at 3, 5; *see also* Doc. 24-3 at 21–22). NCMEC thus connected these latest CyberTips to the previous four received from Google in 2014 and 2015 and forwarded them to law enforcement (Doc. 24-10 at ¶¶ 52, 58).

Search Warrants

In February 2018, shortly after law enforcement received the latest Synchronoss CyberTip, a Magistrate Judge approved search warrants for Crawford's two Google accounts and his Synchronoss account (Doc. 23 at 8). Law enforcement found child-pornography images and videos on Crawford's Synchronoss account (*id.*). Searches of the two Google accounts revealed no child pornography but confirmed that Crawford was the user and that the accounts were suspended due to child-pornography activity (*id.* at 9).

DISCUSSION

Crawford makes two arguments as to why evidence should be suppressed. First, he argues Google and Synchronoss acted as government agents when they searched his accounts without a warrant. Second, he argues the information supporting the Google warrant application was stale.

State Action

First, Crawford argues Google and Synchronoss violated the Fourth Amendment by scanning files uploaded to his accounts and, in Google's case, taking the additional step of viewing his file contents (Doc. 20 at 4–9). But only state action can implicate the Fourth Amendment. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). "[A] private party's search is attributable to the government only 'if the private party acted as an instrument or agent of the Government.'" *United States v. Shepherd*, 646 F. App'x 385, 388 (6th Cir. 2016) (quoting *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989)). Crawford contends NCMEC is a state actor (Doc. 20 at 5–6), and because of its close relationship with Google and Synchronoss, they too are state actors (*id.* at 6–7).

As a preliminary matter, the parties disagree on which test this Court should apply to determine whether a private entity acts as a government agent. This Court agrees with the Government and applies the two-prong test of *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985). *Lambert* provides the appropriate test for criminal cases, like this one, in which a defendant moves to suppress evidence recovered from a search by a private party. *See Lambert*, 771 F.2d at 89 (holding that housekeeper did not act as a government agent in search and seizure of items in a house). *See also Shepherd*, 646 F. App'x at 388–90 (applying *Lambert* and holding that physician did not act as a government agent in scanning patient's body and finding hidden drugs); *United States v. Hardin*, 539 F.3d 404, 419–20 (6th Cir. 2008) (applying *Lambert* and holding that

apartment manager acted as a government agent in searching tenant's apartment). In fact, the Eastern District of Kentucky recently applied the *Lambert* test in a case very similar to this one. *See Miller*, 2017 WL 2705963, at *3 (determining that Google did not act as a government agent by scanning email attachments for child pornography). Although Crawford proposes the nexus test, he provides no authority for applying that test in the context of a Fourth Amendment search (Doc. 20 at 6).

Under the *Lambert* test, Crawford must demonstrate two facts to show that a private entity acted as a government agent for purposes of a Fourth Amendment search: First, the government "must have instigated, encouraged or participated in the search," and second, the private entity "must have engaged in the search with the intent of assisting" the government in its "investigative efforts." *Lambert*, 771 F.2d at 89. *See also Shepherd*, 646 F. App'x at 388.

NCMEC

Crawford's alleged chain of state action first requires NCMEC to be a government agent. The Sixth Circuit has not yet determined whether NCMEC is a government agent, but the Tenth Circuit has ruled that it is. *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) (Gorsuch, J.) (holding that NCMEC is a government agent because it was "endowed with law enforcement powers beyond those enjoyed by private citizens"). In light of *Ackerman*, and because this case can be more easily decided on other grounds, this Court assumes, without deciding, that NCMEC is a state actor.

This assumption does not implicate additional Fourth Amendment concerns because NCMEC did not "exceed[] the scope" of searches by Google and Synchronoss. *Jacobsen*, 466 U.S. at 115. Fourth Amendment protections do not apply if the government merely replicates an earlier private search. *Id.* Here, although NCMEC did not have a warrant when it investigated the

CyberTips, NCMEC viewed only those files that Google already viewed. And when Synchronoss stated it did not view the reported content, NCMEC did not either. NCMEC's further investigation of publicly available information did not violate any reasonable expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

Google and Synchronoss

Crawford argues both Google and Synchronoss acted as government agents when they searched his accounts (Doc. 20 at 7). He asserts the government not only encouraged but required Google and Synchronoss to search his files because a statute requires them to send CyberTips to NCMEC. Providers that discover apparent child pornography on their platforms must report their findings to NCMEC under 18 U.S.C. § 2258A(a). And NCMEC, in turn, is required to make the reports available to law enforcement. 18 U.S.C. § 2258A(c).

But that statute does not require providers to search for child pornography. In fact, the statute specifically states that "[n]othing in this section shall be construed to require a provider to– (1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any communication of any [user, subscriber, or customer]; or (3) affirmatively search, screen, or scan for facts or circumstances" related to online child exploitation. *Id.* § 2258A(f). The statute requires only that a provider report to NCMEC if it discovers apparent child pornography on its platform. *Id.* § 2258A(a). Courts have uniformly rejected the argument that this reporting requirement transforms a provider into a government agent. *See United States v. Miller*, 2017 WL 9325815, at *3 (E.D. Ky. May 19, 2017), *report and recommendation adopted by*, 2017 WL 2705963 (E.D. Ky. June 23, 2017) (collecting cases).

Crawford makes no other argument about how NCMEC encouraged, instigated, or participated in the searches of his accounts, and the record supports none. No evidence suggests NCMEC knew Crawford's accounts existed until after Google and Synchronoss had already searched them. And in those instances where a provider sent several CyberTips on the same account, there is no indication NCMEC encouraged or assisted in the later searches after receiving the initial CyberTip.

As for the second prong -- whether Google and Synchronoss searched with the intent of assisting the government -- those companies monitor their platforms not to assist the government but to further their legitimate business interest in ridding their platforms of abusive content. Where a private party conducts a search for reasons "entirely independent of the government's intent to collect evidence for use in a criminal prosecution, . . . the private party is not an agent of the government." *Hardin*, 539 F.3d at 418 (emphasis omitted) (citation omitted). As stated in an affidavit of Cathy McGoff, Google's Senior Manager of Law Enforcement and Information Security (Doc. 24-11 at ¶ 3):

> Google has a strong business interest in enforcing our terms of service and ensuring that our products are free of illegal content, and in particular, child sexual abuse material. We independently and voluntarily take steps to monitor and safeguard our platform. If our product is associated with being a haven for abusive content and conduct, users will stop using our services. Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.

For similar reasons, Synchronoss also monitors its platform for abusive content "as part of its business practice" (Doc. 24-12 at 2).

The providers' business interest in clearing their platforms of abusive material is independent of the government's interest in investigation and prosecution. Although these interests might overlap in a desire to eradicate child pornography from these platforms, "[s]haring a goal

with the Government is insufficient to transform [a provider] from a private actor into a Government agent." *Miller*, 2017 WL 9325815, at *5 (citation omitted).

Accordingly, neither *Lambert* prong is met here. 771 F.2d at 89. The government did not instigate, encourage, or participate in the searches of Crawford's files. And Google and Synchronoss did not search Crawford's files with the intent of assisting the government in its investigative efforts. Neither Google nor Synchronoss acted as government agents when they searched Crawford's accounts; thus, their conduct did not implicate the Fourth Amendment.

Staleness

Crawford next argues the evidence recovered from his Google accounts should be suppressed because of the delay between his Google uploads in 2014 and 2015 and the search warrant in 2018 (Doc. 20 at 2). On this ground, he challenges only the searches of his Google accounts, not the search of his Synchronoss account.

The Fourth Amendment requires search warrants to be supported by probable cause. Review of a magistrate's probable cause determination is "deferential," *United States v. Bowling*, 900 F.2d 926, 930 (6th Cir. 1990), and reversal is appropriate only if the magistrate exercised discretion arbitrarily, *United States v. Swihart*, 554 F.2d 264, 267–68 (6th Cir. 1977).

Probable cause exists where facts and circumstances indicate "a fair probability that evidence of a crime will be located on the premises of the proposed search." *United States v. Finch*, 998 F.2d 349, 352 (6th Cir. 1993) (citation omitted). A probable cause determination is a common-sense judgment that considers the totality of the circumstances. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "The probable cause inquiry gauges the likelihood that evidence of a crime may presently be found at a certain location." *United States v. Hython*, 443 F.3d 480, 485 (6th Cir. 2006). A

warrant must be supported by "facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." *Sgro v. United States*, 287 U.S. 206, 210 (1932).

"Where the facts occurred too far in the past to give rise to probable cause that evidence of a crime will be found in the location sought to be searched, the facts are said to be stale." 13 A.L.R. Fed. 2d 1. When exactly facts become stale and probable cause expires "is determined by the circumstances of each case . . . and depends on the inherent nature of the crime." *Hython*, 443 F.3d at 485. Staleness cannot be measured "solely by counting the days on a calendar." *United States v. Spikes*, 158 F.3d 913, 923 (6th Cir. 1998). "The passage of time becomes less significant when the crime at issue is ongoing or continuous and the place to be searched is a secure operational base for the crime." *Hython*, 443 F.3d at 485.

Relevant variables to determine staleness include: "(1) the nature of the crime charged; (2) the criminal himself (whether nomadic or entrenched); (3) the item to be seized; and (4) the place to be searched." *United States v. Leaster*, 35 F. App'x 402, 406 (6th Cir. 2002) (citing *Spikes*, 158 F.3d at 923). To review whether the probable cause determination was appropriate here, this Court analyzes these variables below.

The Nature of the Crime

"[C]hild pornography is not a fleeting crime." *United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009). Child-pornography crimes are "generally carried out in the secrecy of the home and over a long period;" thus, "the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography." *United States v. Paull*, 551 F.3d 516, 522 (6th Cir. 2009). Indeed, in *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008), the First Circuit upheld a search warrant where more than three years passed "from the acquisition of the evidence until the warrant application." The court cited the enduring

nature of child pornography, stating that, generally, "customers of child pornography sites do not quickly dispose of their cache." *Id.*

Similarly, here, the gaps in time between tips do not render the information stale. Not only did the information involve child pornography, but the warrant application demonstrated an ongoing pattern of activity that led to a common-sense inference: The person who uploaded the images on the Google accounts in 2014–2015 was the same person who was uploading images on the Synchronoss account in 2017–2018. The CyberTips were generated in August and September 2014 (first Google account), September 2015 (second Google account), October 2017 (Synchronoss account), and January 2018 (Synchronoss account). The two Google accounts were linked by email addresses bearing the name of Crawford's business, and uploads to the accounts came from Internet Protocol (IP) addresses associated with a telecommunications provider in Lima, Ohio (Doc. 24 at ¶¶ 22–23). The later Synchronoss CyberTips listed the uploading device's phone number, and that number matched one that NCMEC found in its investigation of the earlier Google CyberTips (Docs. 24-4 at 3, 5; 24-5 at 3, 6; 24-6 at 3, 5). Publicly available information revealed that the number belonged to Michael Crawford and Countrywide Transport Services in Gomer, Ohio, which is about 10 miles from Lima (Doc. 24-3 at 21–22; Doc. 24-7 at 3).

The later tips from Synchronoss substantiated the earlier tips from Google, and they all involved child pornography. Thus, this factor weighs against staleness.

The Criminal

The warrant application indicates Crawford resided at a Gomer, Ohio, address during the relevant period (Doc. 24-1 at ¶ 31; Doc. 24-7 at ¶ 10). His business was also based in Gomer (Doc. 23 at 7). He was entrenched, not nomadic. This factor too weighs against staleness.

The Thing to be Seized

Digital image files are of "enduring utility," *Spikes*, 158 F.3d at 923, and "[i]mages of child pornography can have an infinite life span," *Frechette*, 583 F.3d at 379. "[D]igital images of child pornography can be easily duplicated and kept indefinitely even if they are sold or traded." *Id.* Indeed, "[i]mages typically persist in some form on a computer hard drive even after the images have been deleted and . . . such evidence can often be recovered by forensic examiners." *United States v. Terry*, 522 F.3d 645, 650 n.2 (6th Cir. 2008). This factor weighs against staleness.

The Place to be Searched

Here, the "places" to be searched were online storage sites -- Google+ Photos and the Synchronoss cloud-storage site. These were places where many files could be stored for indefinite periods of time. This factor also weighs against staleness.

* * *

The warrant application for the Google accounts was not stale. The magistrate did not act arbitrarily in finding probable cause to search Crawford's accounts.

CONCLUSION

The Motion to Suppress (Doc. 20) is denied.

IT IS SO ORDERED.

s/ *Jack Zouhary*
JACK ZOUHARY
U. S. DISTRICT JUDGE

July 16, 2019